КВАНТОВАЯ КРИПТОГРАФИЯ И ЕЕ ПРИМЕНЕНИЕ В СОВРЕМЕННЫХ СИСТЕМАХ БЕЗОПАСНОСТИ

ФРОЛОВ Сергей Иванович
магистрант
Нижневартовский государственный университет
г. Нижневартовск, Россия

В эпоху глобальной цифровизации проблема сохранения конфиденциальности информации приобретает особую актуальность, так как традиционные методы защиты становятся уязвимыми перед новыми видами угроз. Одним из наиболее перспективных направлений обеспечения информационной безопасности является квантовая криптография. В статье рассматриваются основные принципы квантовой механики, которые применяются в квантовой криптографии, а также описываются наиболее известные протоколы квантового распределения ключей (BB84 и E91).
Ключевые слова: квантовая криптография, информационная безопасность, защита данных, BB84, E91.

В эпоху глобальной цифровизации, когда информация является одним из самых ценных ресурсов, проблема сохранения конфиденциальности информации становится всё более актуальной – с каждым днем появляются всё более изощрённые способы кражи данных, однако эксперты по кибербезопасности тоже не стоят на месте и придумывают новые методы борьбы с киберпреступниками. Одним из таких методов является криптография. В данной статье будет рассмотрено одно из направлений современной криптографии, а именно квантовая криптография.

Цель данной статьи – рассмотреть, что представляет собой квантовая криптография, а также ее применение в современных системах безопасности.

Под термином «криптография» понимают технологию шифрования данных таким образом, чтобы зашифрованную информацию нельзя было прочитать, просмотреть или прослушать без дешифровки [1]. Целью криптографии является построение и анализ алгоритмов, которые не позволяют третьим лицам получить доступ к конфиденциальной информации. В современной криптографии выделяется множество направлений, среди которых:

– симметричная – используется один ключ как для шифрования, так и для дешифрования сообщения;

– асимметричная – используется два ключа: приватный и публичный соответственно для шифровки и дешифровки сообщения;

– хэширование – преобразует сообщение в набор символов фиксированной длинны используются для проверки целостности данных;

– цифровые подписи – используются для аутентификации отправителя и обеспечения целостности данных;

– квантовая криптография – использует свойства квантовой механики для создания устойчивых ко взлому криптографических систем.

Рассмотрим подробнее основные принципы квантовой механики, которые используются в квантовой криптографии:

– принцип суперпозиции – согласно данному принципу, результирующий эффект нескольких независимых воздействий есть сумма эффектов, вызываемых каждым воздействием в отдельности [3];

– принцип квантовой запутанности – физическое явление, при котором две частицы настолько сильно связаны друг с другом, что состояние одной частицы не может быть измененено таким образом, чтобы не оказать влияния на другую частицу, даже при условии, что другая частица находится на другом конце вселенной (https://ru.ruwiki.ru (дата обращения 12.12.2024);

– принцип неопределенности гейзенберга – невозможно одновременно точно измерить некоторые пары физических величин, которые связанны друг с другом, например координаты и скорость квантовой частицы [2].

Также одним из основополагающих понятий в квантовой криптографии является понятие поляризации фотона. В классической

электронике нули и единицы кодируются в виде разных потенциалов сигнала либо в виде импульсов определённого направления, в квантовых системах такое кодирование не представляется возможным, поэтому требуется некий параметр фотона, который можно задать при его генерации, а затем с нужной точностью измерить. В качестве такого параметра выступает поляризация.

Со значительными допущениями, поляризацию можно рассматривать как направление фотона в пространстве. Фотон может быть поляризован под углами 0^o, 45^o, 90^o, 135^o. С помощью измерений у фотона можно различить только два взаимно перпендикулярных состояния или базиса (рисунок 1):

– базис «плюс» – фотон поляризован вертикально или горизонтально;

– базис «крест» – фотон поляризован под углами 45 или 135 градусов.

БАЗИС	0	1
+	↑	→
×	↗	↘

Рисунок 1. **Базисы фотона**

Первый протокол, который позволял обмениваться ключами шифрования с помощью фотонов, был предложен канадским физиком-теоретиком Жильем Брассаром и американский физиком-теоретиком и информатиком Чарльзом Беннетом в 1984 г. На данный момент существует несколько протоколов квантового распределения ключей. Наиболее распространенные из них:

– BB84 – протокол Брассара и Беннета. В его основе лежат измерение поляризации фотона и принцип суперпозиции состояний до момента измерения.

– E91 – протокол, созданный в 1991 г. Артуром Экертом. Также предполагает измерение поляризации фотонов, но вместо суперпозиции полагается на квантовую запутанность.

К проблемам квантовой криптографии сегодня можно отнести:

– ограниченную дальность передачи сигналов – текущие системы обеспечивают связь на расстоянии до 100-150 км без ретрансляторов;

– высокую стоимость оборудования – разработка и внедрение квантовых систем требуют значительных инвестиций;

– помехи, вызванные, например, атмосферными явлениями.

Квантовая криптография, хотя и обладает рядом уникальных преимуществ не является абсолютно неуязвимой. Атаки на системы квантового распределения ключей используют недостатки оборудования или ошибки в реализации. Основные виды атак на квантовую криптографию включают:

– Атака на ослепление детекторов: суть данной атаки состоит в том, что на детекторы посылается мощный лазерный импульс, который заставляет их перейти в классический режим работы. В этом режиме детекторы перестают улавливать квантовые свойства фотонов, что позволяет перехватить ключ без обнаружения.

– Атаки с использованием дополнительных степеней свободы фотонов – фотон имеет несколько степеней свободы, таких как поляризация, энергия и время прибытия. Если в алгоритме используется только одна из них, злоумышленник может использовать другие для скрытого извлечения информации, не влияя на детектируемую часть сигнала.

– Социальная инженерия и эксплуатация ошибок операторов – ошибки в настройке

оборудования или неправильное реагирование на сигналы тревоги могут позволить атакующим получить доступ к системе.

Для защиты от приведенных атак, сейчас активно применяются следующие методы:

– Усовершенствование оборудования – квантовая криптография сейчас находится в процессе активного развития, поэтому активно появляются, например, новые типы детекторов, устойчивых к атакам на ослепление.

– Усложнение протоколов: добавление методов верификации и контроля, например, дополнительных проверок аутентификации сигналов.

– Мониторинг квантового канала: анализ статистики сигналов для обнаружения аномалий, вызванных вмешательством.

– Квантовые сети с доверенными узлами: промежуточные узлы могут использоваться для усиления защиты и сокращения длины уязвимого канала.

Сегодня квантовая криптография находит применение в различных отраслях, таких как:

– финансовый сектор – защита транзакций и межбанковских коммуникаций;

– государственные системы – передача информации в органах государственной власти требует максимальной безопасности;

– критическая инфраструктура – энергетические компании и операторы связи внедряют квантовые технологии для защиты своих сетей;

– использование квантовой случайности – генерация истинно случайных чисел с помощью квантовых систем для повышения уровня безопасности криптографических алгоритмов. Это исключает предсказуемость ключей.

В заключении хотелось бы отметить, что в ходе написания статьи были рассмотрены основные принципы квантовой криптографии, ее преимущества и недостатки, а также некоторые виды атак, которым подвержена квантовая криптография.

СПИСОК ЛИТЕРАТУРЫ

1. *Мосенцов С.Н., Буров Н.В.* Введение в квантовую криптографию и квантовое распределение ключей // Фотон-экспресс. – 2021. – С. 4-7.

2. Принцип неопределенности: Ядерная физика в интернете. Проект кафедры общей ядерной физики физического факультета МГУ и отдела электромагнитных процессов и взаимодействия атомных ядер НИИЯФ МГУ. – URL:http://nuclphys.sinp.msu.ru/spargalka/a05.htm (дата обращения: 12.12.2024).

3. Принцип суперпозиции Superposition Principle: Ядерная физика в интернете. Проект кафедры общей ядерной физики физического факультета МГУ и отдела электромагнитных процессов и взаимодействия атомных ядер НИИЯФ МГУ. – URL:http://nuclphys.sinp.msu.ru/enc/e124.htm (дата обращения: 12.12.2024).

QUANTUM CRYPTOGRAPHY AND ITS APPLICATION IN MODERN SECURITY SYSTEMS

FROLOV Sergey Ivanovich
Undergraduate Student
Nizhnevartovsk State University
Nizhnevartovsk, Russia

In the era of global digitalization, the problem of information confidentiality is becoming particularly relevant, as traditional methods of protection are becoming vulnerable to new types of threats. One of the most promising areas of information security is quantum cryptography. The article discusses the basic principles of quantum mechanics, which are used in quantum cryptography, such as superposition, entanglement and polarization of photons, and describes the most famous protocols of quantum key distribution (BB84 and E91).

Keywords: quantum cryptography, information security, data protection, BB84, E91.